"Your logo here"

[Insert Cover Picture]

Government Facilities IED VBIED Tabletop Exercise

Situation Manual

[Insert Date]

[Insert Caveat]

This Situation Manual (SitMan) provides exercise participants with all necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

Photo Courtesy of [insert source]

This page is intentionally left blank.

Exercise Agenda

Start Time	End Time	Activity
7:45 a.m.	8:30 a.m.	Registration
8:30 a.m.	9:00 a.m.	Welcome and Introductions
9:00 a.m.	10:15 a.m.	Module One: Threat
10:15 a.m.	10:30 a.m.	Break
10:30 a.m.	12:00 p.m.	Module Two: Incident and Response
12:00 p.m.	12:15 p.m.	Break
12:15 p.m.	1:30 p.m.	Module Three: Recovery
1:30 p.m.	2:00 p.m.	Hot Wash / Closing Remarks

**All times are approximate*

This page is intentionally left blank.

EXERCISE OVERVIEW

Exercise Name	Government Facilities IED VBIED Tabletop Exercise (TTX)
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a TTX planned for [insert exercise duration] and will focus on [insert scope]. This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP).
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery [Select appropriate Mission Area(s)]
Capabilities	• Economic Recovery • Health and Social Services • Infrastructure Systems • Intelligence and Information Systems • Planning • Public Information and Warning • Risk Management for Protection Programs and Activities • [Insert additional capabilities as necessary]
Objectives	1. Review intelligence and information sharing and dissemination processes in relation to a credible threat to domestic critical infrastructure owners / operators. 2. Assess information sharing capabilities with government sector partners; federal, state, local, tribal, and territorial government departments and agencies; and the public in accordance with applicable plans and procedures. 3. Discuss critical infrastructure stakeholders' emergency preparedness plans and response procedures to a threat-initiated incident and the coordination of activities under the National Incident Management System (NIMS) with local, state, and federal agencies. 4. Examine recovery and business continuity plans following an improvised explosive device (IED) and vehicle-borne IED (VBIED) attack. 5. [Insert additional objectives as necessary]

Threat or Hazard	IED, VBIED
Scenario	A domestic extremist group with nationwide reach targets government facilities.
Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being used, if applicable]
Participating Organizations	[Please see Appendix A.]
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).]

General Information

Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

Exercise Objectives	Capability
Review intelligence and information sharing and dissemination processes in relation to a credible threat to domestic critical infrastructure owners / operators.	✓ Intelligence and Information Sharing
Assess information sharing capabilities with government sector partners; federal, state, local, tribal, and territorial government departments and agencies; and the public in accordance with applicable plans and procedures.	✓ Intelligence and Information Sharing ✓ Public Information and Warning
Discuss critical infrastructure stakeholders' emergency preparedness plans and response procedures to a threat-initiated incident and the coordination of activities under NIMS with local, state, and federal agencies.	✓ Planning ✓ Public Information and Warning ✓ Risk Management for Protection Programs and Activities
Examine recovery and business continuity plans following an IED and VBIED attack.	✓ Economic Recovery ✓ Health and Social Services ✓ Infrastructure Systems ✓ Operational Coordination ✓ Planning
[Insert objective]	✓ [Insert capability aligned to each objective]

Table 1. Exercise Objectives and Associated Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players** have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitators** provide situation updates and moderate the discussion. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
- **Moderators** are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
- **Data Collectors** are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

- Module One: Threat
- Module Two: Incident and Aftermath
- Module Three: Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

Exercise Guidelines

- This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.

- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your jurisdiction's / organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
- The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page is intentionally left blank.

Module One: Pre-Incident Information Sharing

Scenario

[Insert Event Date – 45 days]: [Insert time]

Based on recent incidents in the United States and abroad, along with increased intelligence reporting calling for similar attacks, the Secretary of Homeland Security, in coordination with other federal entities, issues an "Elevated" threat alert through the National Terrorism Advisory System (NTAS), warning of a credible terrorist threat against government facilities in the United States. There is no specific information at this time that would warrant the release of an "Imminent" threat alert.

The alert follows a period of heightened domestic conflict and states the threat is from domestic terrorist groups in the United States with ties to anti-government extremist organizations. These groups are focused on government facilities. Additionally, the alert indicates these groups may be developing plans to use IEDs concealed in backpacks and duffle bags. The alert is to remain in place for three months, ending on [insert date].

The Department of Homeland Security (DHS) sent the alert to its partners in the Government Facilities Sector.

Discussion Questions

1. What internal information sharing and dissemination processes does your organization currently use for this type of threat information?
2. How would your agency or organization expect to receive information about a credible threat?
    a. What steps does your agency or organization take once they receive notice of a credible threat?
3. Does your agency or organization receive NTAS alerts?
    a. What about Suspicious Activity Report (SAR) Bulletins?

4. How would your organization receive intelligence and protective measure information concerning this type of threat?
    a. What security organizations would you communicate with (e.g., Federal Protective Service [FPS], other agency-specific or local law enforcement agencies, security agencies, Federal Bureau of Investigation [FBI], etc.)?
    b. What is the role of the Facility Security Committee (FSC) or Federal Executive Board in sharing threat and protective measure information?
    c. Does your organization maintain a relationship with your Interagency Security Committee (ISC) Regional Advisor, Protective Security Advisor (PSA), or other members of the CISA Regional Office? If so, do you have a rapid means of contacting them?
    d. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal?
5. Would your facility adjust its security measures after the issuance of the NTAS elevated threat alert? If so, how?
6. If there is "suspicious behavior" observed at government facilities, how do the facilities report this information locally and within the sector?
    a. Are trends in suspicious behavior reports tracked across government facilities nationwide?
    b. Is your organization aware of the "If You See Something, Say Something™" campaign or the Nationwide Suspicious Activity Reporting Initiative (NSI)?
    c. Would you share this threat information with international industry partners?
7. What risk mitigation or protective actions would you implement following this alert?
    a. Would you take any additional measures to monitor for suspicious activity?

Scenario Update

[Insert Event – 14 days]: [Insert time]

During an arrest stemming from a traffic stop, a law enforcement officer in [insert location] discovered what were believed to be bomb-making materials and anti-government propaganda. Local law enforcement's search of the suspect's residence finds surveillance materials, including maps, photographs, and documentation, that suggest planned attacks at several local government buildings.

Further investigation leads local law enforcement to determine that there are multiple planned attacks targeting communities throughout the U.S.

Discussion Questions

1. How does your organization triage the threat information you receive (e.g., formal reporting, rumors, social media) for further dissemination within your organization?
2. What information or warnings about the elevated threat level are being released to the public?
    a. Do you have a public information officer (PIO)?
    b. Who is responsible for the initial messaging?
    c. How quickly is information being released?
    d. What methods are being used to distribute information?
    e. What should the content of the messaging be?
    f. Are businesses or other organizations providing their own messaging to their employees?
    g. How are messages coordinated across the different agencies and organizations?
3. What resources are used to disseminate threat information both internally and to the public?
    a. What notification capabilities (e.g., alerts, email, telecom, text message, special tools) do you use to share information and communicate protective measures appropriately with tenants, security organizations, internal personnel, contractors, vendors, and surrounding communities?
    b. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing, such as religious customs that prohibit use of electronic communication during specific times?

   i. If so, how will threat-based alerts and notifications be distributed to community members who follow religious customs that prohibit the use of electronic communication during specific times?

4. Given current and established information sharing procedures, what types of official information are the most useful (e.g., immediate information versus analyzed information) to your organization?
   a. Does your organization perform independent analysis on information provided? If so, describe the process.
5. If your organization receives information related to potential threats against your facilities and personnel, how would you communicate this information to the appropriate security entities (e.g., FPS, local law enforcement agencies, joint terrorism task force [FBI, your ISC Regional Advisor, PSA, or other members of the CISA Regional Office, etc.)?
6. Given evidence of a credible threat to government facilities, does your organization review your emergency response plans (e.g., facility security plans, occupant emergency plans, emergency action plans, continuity of operations plans [COOP], or other appropriate plans or documents)?
7. Is there initial and ongoing training for security personnel on IED awareness and recognition?
8. Are security personnel trained in the difference between an "abandoned item" and a "suspicious package?"
9. What protective security measures or recommendations, if any, will be employed at our organization based on this threat?
   a. Does your facility have an FSC or similar organization responsible for making security and risk decisions for the facility?
   b. Do you coordinate protective measure implementation with any other organization within government facilities or with government entities such as FPS, other agency specific or local law enforcement agencies, ISC Regional Advisor, PSA, or other members of the CISA Regional Office?
   c. What are some procedural changes your facility could make to temporarily increase its protective posture?
   d. How are the protective measures government facilities have put in place communicated back to the tenants, contractors, local first responders, and the department / agency?
   e. How useful are the information bulletins and advisories DHS provides (e.g., a joint intelligence bulletin [JIB]) that recommend protective measures)?

Module Two: Incident Response

Scenario

[Insert Location]

[Insert Month, Day, Year]: [Insert time]

It is approaching mid-morning and [insert name of government facility] is already packed with people conducting their business. A group of people wait to be screened for entry into the facility when an individual approaches the federal facility and causally places a backpack next to the line before anyone has a chance to report the suspicious package. Moments later, an explosion rips through the screening area, the blast propels shrapnel and debris into surrounding areas. In the confusion, people frantically flee the area, resulting in additional injuries from traversing the mangled building that is now littered with debris.

First responders quickly arrive and attempt to secure the scene and triage the injured. They initially estimate at least [insert number] killed and many more injured. Callers quickly overwhelm 9-1-1 dispatch, reporting the explosion and survivors calling for help. Live-streaming video and images from the scene are being uploaded to multiple social media sites.

Discussion Questions

1. What are your organization's information sharing responsibilities during the response to the incident?
2. What formal information sharing processes would your organization use at this point?
3. What resources are used to disseminate information?
    a. What notification capabilities (e.g., alerts, email, telecom, text messages, special tools) do you use to share information and appropriately communicate protective measures implementation with tenants, security organizations, etc.?
4. Do your existing plans, policies, and procedures address counter-IED (C-IED) considerations?
    a. If not, are you familiar with the resources available through the CISA Office of Bombing Prevention to assist in incorporating C-IED measures into planning efforts?
5. What actions are on-scene security and law enforcement taking in response to the bombing attack?
    a. What information would be conveyed to the facility employees and security personnel?

b. How would this information be shared?

6. How quickly could additional support, such as K-9, bomb squads, or state and federal resources be brought to the scene?
7. What are the authorities, federal / state / local laws, or protection capabilities your facility or law enforcement partners employ in immediate response, investigation, or prosecution of civil or criminal penalties?
    a. Does your agency or department have UAS detection capabilities? How is it integrated into your emergency operations center (EOC) to ensure synchronization of response efforts?
8. What are crowd control and / or evacuation procedures for an incident of this type?
    a. Who is responsible for activating the evacuation procedures?
    b. Is there a specified location for evacuees?
        i. Would the location be searched for secondary device(s) prior to evacuation?
        ii. Would this location change in the event of inclement weather?
        iii. Are there secondary or tertiary rally points in case the primary point is a part of the incident or evacuees overwhelm it?
    c. Are operations staff trained in the crowd control / evacuation procedures?
    d. Are local responders familiar with your emergency procedures?
        i. Are they trained for scenarios like this?
    e. How are the employees notified of the evacuation plan once it is set in motion?
9. Would your organization take accountability for the staff working at the building, and, if so, how?

Scenario Update

Location: [Insert Local Government Office Building]

[Insert Month, Day, Year]: [Insert Initial Incident + 40 minutes]

The morning's events significantly raised the anxiety level of the employees at the [insert name of government office building]. Some employees heed the warnings of security officials and remain in the building, while others decide to leave the premises. Security personnel prevent anyone currently outside the building from entering as they attempt to maintain a secure perimeter.

A car pulls up next to the main entrance of [insert name of government office building]. As a police officer approaches the vehicle to direct it away from the building, the vehicle explodes. The explosion creates a massive fireball and throws glass, metal, and asphalt into the air. The blast carves a large hole in the side of the building by the front entrance and shatters windows in the surrounding buildings.

Calls overwhelm the local 9-1-1 dispatch, which was already operating at peak capacity following the first detonation. Cellular phone service is limited as networks are receiving more traffic than they can handle. People begin pouring out into the streets from nearby buildings in confusion.

There are unknown casualties resulting from the vehicle-borne IED (VBIED), which has also generated major infrastructure damage in the area, including ruptured gas and water mains and area power outages.

Discussion Questions

1. Who is the on-site security organization? What other security or law enforcement entities might also be on-site?
2. How would overwhelmed local first responders impact on-site security?
3. Who is responsible for coordinating the risk communications message for your organization?
4. What are the key messages concerning the continuing credible threat to your organization and stakeholders?
    a. Is the message coordinated with the building tenants and their department or agency?
    b. If so, what is the process for coordinating this message?
5. What protective security measures will be employed at your organization following these domestic attacks?
6. What command and control considerations would be taken at this point in the response?

7. Would fire and emergency medical services personnel be delayed in entering the scene to assist the injured? Why or why not?
    a. What are the potential delays that could result?
        i. How would the delays be mitigated?
8. How quickly are messages being released to the public?
    a. Who is responsible for this type of messaging?
    b. How are they being released?
    c. How are messages coordinated across the different agencies and organizations?
9. How does your facility handle incoming calls from people searching for loved ones?
10. What is the role of private sector stakeholders in this command structure?
    a. Are they trained on incident command procedures?
    b. Is there cross-training among public and private sector partners?
    c. Does your organization have representation within the EOC or the Unified Command?
11. What plans or procedures exist to work with those with access and functional needs?

MODULE THREE: RECOVERY

Scenario
[Insert Location]

[Insert Incident + 2-3 Days]: [Insert Time]

Several days have passed after the attacks at [insert name of service facility] and [insert name of government office building]. Law enforcement organizations are continuing their investigations and have identified that the attacks were carried out by an anti-government extremist organization. Both facilities are still closed because of the ongoing investigation and infrastructure instability. Initial damage assessments have found that there is significant cosmetic and structural damage because of the explosion.

Multiple locally appointed and elected leaders from various departments, as well as media, are inquiring about the status of operations and are asking for detailed reports on the incident for use in investigations. Employees are overwhelming departmental email listservs inquiring about the cause of the incident and what immediate protective measures are being taken to ensure their safety.

Social media is rampant with rumors and speculation about the incidents. Multiple news outlets continue to dispatch reporters to the scenes to interview witnesses and capture footage of the area.

Discussion Questions

1. Does your organization maintain a business continuity or rapid recovery plan that addresses this type of incident?
    a. What could be the impact of law enforcement designating the facility, or portions of your facility, an active crime scene?
        i. How will law enforcement coordinate facility issues related to the investigation with owners / operators?
        ii. How will the facility address any impediments to operations?
    b. What plans are there for continuing operations if the facility suffers significant structural damage?
    c. Does your organization have a formal devolution plan?
2. What are the facility's priorities related to continuity and recovery?

   a. What type of potential liability issues from this incident would facility managers be addressing at this point?

3. What local, state, or federal resources are available to assist in recovery or business continuity?
4. Will law enforcement be able to estimate the timeframe required for the facilities to remain a crime scene?
5. What post-incident recovery activities might be needed for employees, their families, and operations (e.g., reunification, psychological resources, first aid, etc.)?
   a. How is information communicated to personnel and families during the days following the incident? How will personnel accountability and communication be coordinated?
   b. What type of counseling for employees and family members is available?
   c. What type of financial assistance or benefit programs are available for employees if the facility is shut down on a temporary basis?
   d. What is the procedure if injuries received on the job (in this case by an IED / VBIED) hospitalized an employee?
   e. What is the process for assisting the family members of a deceased employee?
6. How would memorials be coordinated for those who perished during the attack?
   a. Does the city have any laws restricting the duration or location of memorials?
7. What messaging would be sent out to the community about this type of situation?
   a. What about messaging to other government departments and agencies?
8. Who will be responsible for coordinating responses for any resultant governmental inquiries?
9. What is the plan to handle the extended media attention from local and national outlets?
   a. What specific plans and procedures are in your emergency operations plans (EOP)?
   b. What separate plans do you have to handle social media?

APPENDIX A: EXERCISE PARTICIPANTS

Participating Private Sector Organizations
[Insert private sector participants]

Participating Local Organizations
[Insert local participants]

Participating State Organizations
[Insert state participants]

Participating Federal Organizations
[Insert federal participants]

Other Participating Organizations
[Insert other participants]

Other Participating Organizations

This page is intentionally left blank.

APPENDIX B: RELEVANT PLANS

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

APPENDIX C: ACRONYMS

Acronym	Term
AAR	After-Action Report
C-IED	Counter-Improvised Explosive Device
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
CTEP	CISA Tabletop Exercise Package
DHS	Department of Homeland Security
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
EPT	Exercise Planning Team
FBI	Federal Bureau of Investigation
FPS	Federal Protective Service
FSC	Facility Security Committee
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
IED	Improvised Explosive Device
IP	Improvement Plan
ISC	Interagency Security Committee
JIB	Joint Intelligence Bulletin
NIMS	National Incident Management System
NSI	Nationwide Suspicious Activity Reporting Initiative
NTAS	National Terrorism Advisory System
PIO	Public Information Officer
POC	Point of Contact
PSA	Protective Security Advisor
SAR	Suspicious Activity Report
SitMan	Situation Manual
SME	Subject Matter Expert
TTX	Tabletop Exercise

Acronym	Term
VBIED	Vehicle-Borne Improvised Explosive Device